APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/509,067	05/18/2005	Vincent Finkelstein	0579-1070	1373

466   7590   01/23/2009
YOUNG & THOMPSON
209 Madison Street
Suite 500
ALEXANDRIA, VA 22314

EXAMINER
REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
01/23/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>24 September 2004</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-21</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-21</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>24 September 2004</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

        1.☒ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date <u>9/24/04</u>.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

Priority

1.   Acknowledgment is made of applicant's claim for foreign priority under 35

U.S.C. 119(a)-(d).

Information Disclosure Statement

2.   The information disclosure statement (IDS) submitted on September 24, 2004 is

in compliance with the provisions of 37 CFR 1.97. Accordingly, the information

disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by
> another filed in the United States before the invention by the applicant for patent or (2) a patent
> granted on an application for patent by another filed in the United States before the invention by the
> applicant for patent, except that an international application filed under the treaty defined in section
> 351(a) shall have the effects for purposes of this subsection of an application filed in the United States
> only if the international application designated the United States and was published under Article 21(2)
> of such treaty in the English language.

4.   Claims 1-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Ellison

et al, U.S. Patent 7,082,615.

As per claim 1, it is taught of a method of automatic validation of a computer

program able to access secure memory (MS) and non-secure memory (MNS), the

program using at least one encryption function (DES) and at least one decryption

function (DES-1), characterized in that it comprises a verification step (E340) which

verifies that: any function adapted to read data from said secure memory (MS) and to

produce data in said non-secure memory (MNS) is an encryption function; and any data

produced by said decryption function is stored in said secure memory (MS)(col. 6, line

44 through col. 7, line 27).

As per claim 2, it is disclosed of a validation method according to claim 1,

characterized in that said program also uses at least one non-cryptographic function,

said non-cryptographic function being chosen from a logic function, a random number

generation function and an integrity check function (col. 8, lines 47-65 and col. 9, lines

6-24).

As per claim 3, it is taught of a validation method according to claim 2,

characterized in that any data produced by said non-cryptographic function from data

read in said secure memory (MS) is stored in said secure memory (MS)(col. 6, line 44

through col. 7, line 27).

As per claim 4, it is disclosed of a validation method according to claim 1,

characterized in that, the computer program being in source code, the method

comprises, before said verification step (E340), a step (E300) of compilation of said

source code into binary script (EXE), said verification step (E340) being effected on the

binary script (EXE) generated in this way (col. 8, lines 47-65 and col. 9, lines 6-24).

As per claim 5, it is taught of a validation method according to claim 1, characterized in that said computer program is a sensitive data generation program (col. 6, line 44 through col. 7, line 27).

As per claim 6, it is disclosed of a validation method according to claim 1, characterized in that said computer program is a sensitive data transformation program (col. 6, line 44 through col. 7, line 27).

As per claim 7, it is taught of a validation method according to claim 1, characterized in that each function used by said computer program is associated with at least one operating mode that defines at least one rule governing access to said memories, said operating mode being stored in a verification table (TV) used during said verification step (E340) (col. 6, line 44 through col. 7, line 27).

As per claim 8, it is disclosed of a validation method according to claim 7, characterized in that it further comprises a step (E310) of allocation of said secure memory (MS) and said non-secure memory (MNS); a step of loading into a working memory a verifier program for said binary script (EXE), said verifier program being adapted to implement said verification step (E340); and a step (E305) of loading said binary script (EXE) into said working memory (col. 6, line 44 through col. 7, line 27; col. 8, lines 47-65; and col. 9, lines 6-24).

As per claim 9, it is taught of a compiler characterized in that it is adapted to implement a validation method according to claim 1 (col. 8, lines 47-65 and col. 9, lines 6-24).

As per claim 10, it is disclosed of a method of executing a computer program adapted to access secure memory (MS) and non-secure memory (MNS), the program using at least one encryption function (DES) and at least one decryption function (DES-1), characterized in that a verification step (E340) conforming to claim 1 is executed before the execution (E420) of each function of said program (col. 6, line 44 through col. 7, line 27; col. 8, lines 47-65; and col. 9, lines 6-24).

As per claim 11, it is taught of the use of the execution method according to claim 10 to transform or generate sensitive data (col. 6, line 44 through col. 7, line 27).

As per claim 12, it is disclosed of the use of the execution method according to claim 10 to customize microcircuit cards (col. 7, lines 59-63).

As per claim 13, it is taught of an integrated electronic circuit characterized in that it is adapted to implement a validation method according to claim 1(col. 8, lines 47-65 and col. 9, lines 6-24).

As per claim 14, it is disclosed of a microcircuit card characterized in that it comprises an integrated electronic circuit according to claim 13 (col. 7, lines 59-63).

As per claim 15, it is taught of a computer system characterized in that it comprises an electronic integrated circuit according to claim 13 (col. 7, lines 59-63).

As per claim 16, it is disclosed of a secure operating system adapted to implement a validation method according to claim 1 (col. 8, lines 47-65 and col. 9, lines 6-24).

As per claim 17, it is taught of a microcircuit card characterized in that it comprises an operating system according to claim 16 (col. 3, lines 9-25).

As per claim 18, it is disclosed of a computer system characterized in that it comprises an operating system according to claim 16 (col. 3, lines 9-25).

As per claim 19, it is taught of a device for validating a computer program adapted to access secure memory (MS) and non-secure memory (MNS), the program using at least one encryption function (DES) and at least one decryption function (DES-1), characterized in that it comprises a verifier program adapted to verify that: any function adapted to read data from said secure memory (MS) and to produce data in said non-secure memory (MNS) is an encryption function; and any data produced by said decryption function is stored in said secure memory (MS)(col. 6, line 44 through col. 7, line 27).

As per claim 20, it is disclosed of a validation device according to claim 19, characterized in that the verifier program is adapted to effect said verifications on the basis of a binary script (EXE) obtained by compilation of said computer program (col. 8, lines 47-65 and col. 9, lines 6-24).

As per claim 21, it is taught of a computer system comprising a secure operating system characterized in that it comprises means for compiling a computer program in binary script (EXE); means for loading said binary script (EXE) into a working memory; means for allocating secure memory (MS) and non-secure memory (MNS); and a validation device according to claim 19 (col. 6, line 44 through col. 7, line 27; col. 8, lines 47-65; and col. 9, lines 6-24).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Thursday, 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher A. Revak/
Primary Examiner, Art Unit 2431